White Paper

Intel® Centrino® 2 with vPro™ Technology

Intel® Core™2 Processor with vPro™ Technology

Intel® Centrino® 2 with vPro™ Technology and Intel® Core™2 Processor with vPro™ Technology

Best for Business: Security and Manageability on the Chip

The latest notebook and desktop PCs with Intel® vPro™ technology build on proven capabilities to enable greater proactive security, enhanced maintenance, and improved remote management both inside and outside the corporate firewall:

- Intel® Centrino® 2 with vPro™ technology-based notebooks
- Intel® Core™2 processor with vPro™ technology-based desktop PCs

These notebook and desktop PCs deliver down-the-wire security and manageability capabilities – even if the PC's power is off, the operating system (OS) is unresponsive, software agents are disabled, or hardware (such as a hard drive) has failed. With a secure tunnel for communications both inside and outside the corporate firewall, information technology (IT) managers can securely maintain, update, and repair PCs even on an open wired LAN outside the corporate firewall. Remote configuration helps information technology (IT) managers deploy thousands of notebook and desktop PCs without making a deskside visit. In addition, new, optional Intel® Anti-Theft Technology (Intel® AT) for notebooks can help protect encrypted data from unauthorized access if a system is lost or stolen. Notebook and desktop PCs also support OS and application streaming, as well as traditional virtualization with multiple OSs – and do so faster and in a more secure, trusted environment. The latest PCs with Intel vPro technology deliver significantly improved 64-bit multi-core performance for compute-intensive tasks – and include fully integrated powerful graphics support – all in a power-efficient package that is Microsoft Windows 7* ready.

Table of Contents

Executive Summary

Proven Intel® vPro™ technology is built into notebook and desktop PCs to extend the reach and functionality of the management console and meet your critical IT challenges. This hardware-based technology delivers security and manageability on the chip through:

- Intel® Centrino® 2 with vPro™ technology-based notebooks.
- Intel® Core™2 processor with vPro™ technology-based desktop PCs.[1]

IT technicians can now protect, maintain, and manage notebook and desktop PCs – even if the PC's power is off, its OS is unresponsive, hardware (such as a hard drive) has failed, or software agents are missing.[1] IT administrators can quickly identify and contain more security threats, remotely maintain PCs virtually anytime, take more accurate hardware/software inventories, quickly resolve more software and OS problems down-the-wire, and accurately diagnose hardware problems – all without leaving the service center. Technicians can even securely maintain, update, troubleshoot, repair, and receive alerts from notebook and desktop PCs that are on an open wired LAN outside the corporate firewall.[2] With new Intel® Anti-Theft Technology[3] (Intel® AT) for notebooks, IT administrators can also be more assured that encrypted data is better protected from unauthorized access if a system is lost or stolen. For Intel Centrino 2 with vPro technology-based notebooks, optional, integrated WiFi/WiMAX allow users to experience broadband connectivity on the go for wireless access beyond today's hot spots.[4]

With Intel vPro technology, IT managers benefit from lower support costs, easier and more automated maintenance, improved security, increased compliance and more accurate inventories. In turn, companies can see significantly fewer service depot and deskside visits, and less interruption to business.

The latest Intel-based notebook and desktop PCs also deliver significantly improved performance for compute-intensive applications and multitasking all in a power-efficient package that is Microsoft Windows 7* ready. These PCs also include hardware-based capabilities that enable next-generation standard practice virtualization use cases, such as OS and application streaming, as well as traditional virtualization in a faster, separate environment.

IT organizations can now spend less time on routine tasks, and can focus resources where they are most needed.

Notebook and desktop PCs with Intel® vPro™ technology

Notebook and desktop PCs with Intel vPro technology deliver down-the-wire security, enhanced maintenance, and remote management designed right into the chip.

Today's IT challenges

Information technology (IT) managers have a critical need for capabilities that make it easier to secure and manage notebook and desktop PCs anywhere, anytime. Key IT challenges today include:

- A dramatic increase in data breaches, identity theft, malicious attacks on PCs, and computer theft.
- A critical need to reduce user downtime caused by malicious attacks, maintenance IT work, diagnostics and repair, updates, upgrades, and other IT tasks.
- Financial and legal pressure to accurately inventory assets.
- Escalating demand for IT services — especially for mobile PCs — that strain IT budgets.

Typical security and management solutions are software-based. Unfortunately, IT cannot typically use software-based solutions to protect or manage a PC whose power is off, OS is unresponsive, or management agents are missing. They also can't securely manage or protect a notebook or desktop PC in certain types of remote locations, such as over an open wired LAN outside the corporate firewall.

There is an increased need to establish secure, well-managed environments for both mobile and desktop PCs; however, the cost of managing PCs has become a significant percentage of the Total Cost of Ownership (TCO) of technology. A critical capability that has proven to help IT do more with the resources they have is the ability to protect and remotely manage both notebook and desktop PCs, regardless of power state, wired or wireless state, the state of the OS, or the location of the PC.

Security and remote manageability built into the chip

Designed for business, notebook and desktop PCs with Intel vPro technology deliver the hardware-based capabilities IT organizations need to meet the increasing demands for their services.

- Intel® Centrino® 2 with vPro™ technology for notebooks.
- Intel® Core™2 processor with vPro™ technology for desktop PCs.

Challenge	Solution with Intel® vPro™ technology
Systems unmanageable when powered down	Remotely and securely monitor and manage PCs anytime: • Access the PC even if PC power is off, the OS is unresponsive, management agents are missing, or hardware (such as a hard drive) has failed. • Access critical system information (asset information, event logs, BIOS information, etc.) virtually anytime, even if PC power is off, to identify systems that need maintenance or service. • Remotely and securely power up PCs for maintenance and service.
Unsecured communications with PCs	More securely communicate with notebook and desktop PCs both inside or outside the corporate firewall: • Access PCs through a secure, out-of-band communication channel inside the corporate firewall. • Establish a secure tunnel to PCs on a wired open LAN even outside the corporate firewall.
Spiraling and costly deskside visits	Significantly reduce deskside visits with: • Remote remediation, even if management agents are missing or the OS is unresponsive. • Remote problem resolution, even if the OS is unresponsive or hardware (such as a hard drive) has failed.
Unprotected assets	Protect assets better: • Remotely power up PCs anytime to help ensure more complete saturation for patching and other updates. • Built-in, programmable system defense filters and agent-presence checking for automated, hardware-based protection against viruses and attacks. • Built-in, programmable triggers and responses in notebooks to protect data and the PC after loss or theft of the system.
Lack of configuration compliance	Ensure compliance: • Remote inventory and agent presence checking as a hardware-based, automated, policy-based service.
Costly and time-consuming manual inventories	Eliminate virtually all manual inventories: • Accurate, remote asset inventories, even if PCs are powered off or management agents are missing.
Undiscoverable assets	Discover virtually all PCs: • Persistent device ID available anytime, even if PC power is off, the OS has been rebuilt, hardware or software configuration has changed, or the hard drive has been reimaged.

Proven technology for critical challenges

The latest notebook and desktop PCs with Intel vPro technology are delivered with proven hardware-based technology designed to address the top IT challenges in security and manageability.[1] These notebook and desktop PCs deliver even more powerful security, maintenance, and management capabilities. These PCs also offer full, secure remote deployment to help IT managers eliminate deskside visits during large roll-outs.

Access the PC anytime, anywhere

The hardware-based capabilities of Intel vPro technology let authorized technicians remotely access PCs that have traditionally been unavailable to the management console. Technicians can use Intel vPro technology to manage the wired or wireless notebook or wired desktop PC even if PC power is off, the OS is unresponsive, hardware (such as a hard drive) has failed, or management agents are missing. Best of all, with a secure tunnel for communications even outside the corporate firewall, technicians can remotely maintain, update, and repair both notebook and desktop PCs even on an open wired LAN, at sites that don't have a proxy server.

Intel vPro technology: Summary of benefits

The new notebook and desktop PCs are designed for business in an advanced, energy-efficient package with 64-bit multi-core performance and 64-bit integrated graphics support that is Microsoft Windows 7 ready. These PCs deliver:

- **Security —** so you can help ensure compliance down-the-wire on virtually all PCs with Intel vPro technology; ensure that third-party security software is available when needed; remotely identify viruses, worms, and other threats faster; and stop those threats more effectively. Intel vPro technology supports 802.1x, Cisco Self-Defending Network* (Cisco SDN), or Microsoft Network Access Protection* (Microsoft NAP), so you can maintain and manage these PCs even in secure network environments. Intel® Anti-Theft Technology (Intel® AT) for notebooks can help prevent unauthorized access to encrypted data if a notebook is lost or stolen.
- **Improved maintenance —** so you can streamline processes, increase automation, and dramatically improve technician efficiencies for monitoring and maintenance of all PCs with Intel vPro technology during a scheduled maintenance cycle.
- **Remote problem-resolution —** so you can accurately diagnose hardware problems and troubleshoot and resolve more software and OS problems, including OS rebuilds, without leaving the service center.
- **Remote inventory and discovery —** to help you eliminate manual inventories, improve compliance with government and industry regulations, and reduce management costs.
- **Remote configuration during deployment —** so you can remotely configure both notebook and desktop PCs without a deskside visit.
- **Energy savings —** companies are finding that Intel vPro technology is helping deliver substantial power savings by letting IT be more effective in power management. IT can use Intel vPro technology to securely and remotely power systems up for maintenance and management anytime, so PCs can be powered down when not in use.

Combined with third-party management applications, the new generation of Intel vPro technology allows IT administrators to simplify maintenance, eliminate a significant number of deskside visits, reduce overspending on existing resources, and minimize interruptions to business.

What's New...

Advancements in Intel vPro technology include the integration of new capabilities into both notebook and desktop PCs. Additional features have been added to improve security and manageability both inside and outside the corporate firewall. Along with significant performance gains over previous generation PCs, key advancements in the latest PCs with Intel vPro technology include:

- Support for Microsoft NAP (as well as existing support for 802.1x, PXE, and Cisco SDN) in both notebook and desktop PCs, so you can use out-of-band management even in secure network environments.
- Secure tunnel for communications with the management console for both notebook and desktop PCs operating on an open, wired LAN outside the corporate firewall.[2]
- PC-initiated secure communications to the IT console for wired PCs over an open LAN, outside the corporate firewall, for specific requests for help or service:[2]
  - Hotkey feature that lets a user quickly establish a secure connection from PC to management console — whether from inside or outside the corporate firewall — for help or system servicing.[2]
  - PC-initiated request for remote, prescheduled maintenance, even if the notebook or desktop system is asleep or powered down.[2]
  - Automated remote IT alert, so the PC can automatically and securely report critical events to the management console — even from outside the corporate firewall.[2]
- Intel Anti-Theft Technology, an optional feature for notebooks, which provides IT with programmable triggers and "poison pill" responses that can be used to disable the PC and/or prevent unauthorized access to encrypted data if a notebook is lost or stolen.

PCs with Intel® vPro™ technology[1]

Notebook and desktop PCs with Intel® vPro™ technology deliver validated, fully integrated systems that help IT organizations improve security and remote management for both wired and wireless systems. These PCs are based on the Intel® Core™2 processor to give users excellent 64-bit performance for compute-intensive applications and multitasking while delivering enhanced capabilities for IT, a unique combination of capabilities, only from Intel.

Intel® Centrino® 2 with vPro™ technology for notebooks	Intel® Core™2 processor with vPro™ technology for desktop PCs
45nm Intel® Core™2 Duo processor T9000, P9000, P8000, SP9000, SL9000, SU9000 series; and 45nm Intel® Core™2 Quad processor Q9000 series[6]	45nm Intel® Core™2 Duo processor E8000 series; 45nm Intel® Core™2 Quad processor Q9000 series[6]
Intel® Active Management Technology[1] (Intel® AMT), release 4.0 or 4.x	Intel® Active Management Technology[1] (Intel® AMT), release 5.0 or higher
Intel® 82567LM-3 Gigabit network connection	Intel® 82567LM Gigabit network connection
Support for 802.11a/g/n wireless protocols[7]	
WiFi and optional WiMAX support, with Intel WiMAX/WiFi Link 5350 and Intel WiFi Link 5300	
Optional Intel® Anti-Theft Technology[a,3] (Intel® AT)	
Intel® Virtualization Technology[5] (Intel® VT) including Intel® VT for Directed I/O, and support for OS and application streaming	
Intel® Trusted Execution Technology[8] (Intel® TXT)	
Support for Cisco Self-Defending Network* (Cisco SDN*),Microsoft Network Access Protection* (NAP), and PXE (preexecution environment)	
Support for 802.1x	
64-bit enabled[9]	
Execute Disable Bit[10]	
Industry-standard TPM 1.2[11]	
Intel® Stable Image Platform Program (Intel® SIPP)[12]	
Windows Vista* and Windows 7* ready	
Integrated support for 64-bit graphics, including support for Windows Aero* interface	
Windows Vista* BitLocker*-ready[13]	

[a] Intel AT will be available to the market before it is incorporated into the Intel® Stable Image Platform Program (Intel® SIPP). Intel AT is expected to be included in Intel SIPP in 2010.

- Auditor oversight for protected event logs, in addition to the traditional ability for a system administrator to view and/or erase standard logs.
- Virtualization support, including for next-generation OS and application streaming models into secure virtual environments, on both notebook and desktop PCs via Intel® Virtualization Technology (Intel® VT).[5]

Best for business:
Remote maintenance, management, and security virtually anytime

Intel vPro technology capabilities are available virtually anytime, even if:

- PC power is off.
- OS is unresponsive.
- Management agents are missing.
- Hardware (such as a hard drive) has failed.

Most capabilities are available even for wired PCs outside the corporate firewall, while some capabilities are also available for wireless notebooks in the presence of a host OS-based VPN. IT administrators now have more control where they need it: at the remote IT console.

Combined with third-party management tools such as management consoles and scripting, Intel vPro technology makes it easier to secure, maintain, and manage PCs. The results can be dramatically reduced site visits; substantially improved technician efficiencies; streamlined diagnostics, repair, and remediation; and more automation of processes. In turn, this can help IT managers free up resources for other projects.

Figure 1 shows an example of how notebook and desktop PCs can be remotely managed regardless of PC power state or the state of the OS.

Refer to the discussion, Managing wired or wireless PCs, on page 10, for a list of capabilities available in wired and wireless states, active and sleep states, and various power states.

Secure and manage PCs outside the corporate firewall

Intel vPro technology delivers both new and proven capabilities to secure and maintain PCs even when they are outside the corporate firewall. For example, these notebook and desktop systems support a "client-initiated" or PC-initiated secure tunnel for communication outside the corporate firewall for specific requests for help or service.

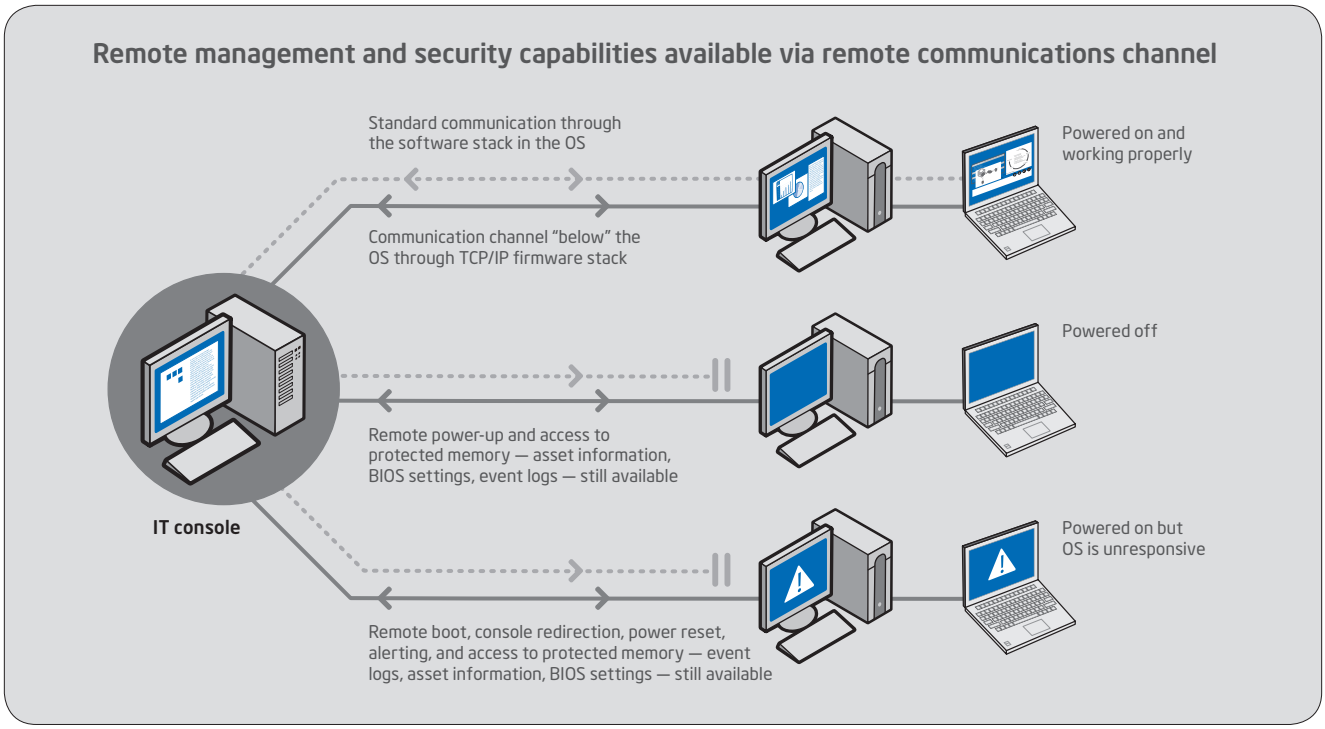

Figure 1. All capabilities are available for notebook and desktop PCs wired and on AC power. Hardware-based communication and capabilities are available virtually anytime for wired, AC-powered PCs. All key capabilities are also available for wireless notebooks within the corporate network even if the PC is powered off, its OS is inoperable, or the notebook is asleep.[14] (Some capabilities are active only when the notebook is awake and performing a particular task.) All capabilities are available for wired PCs outside the corporate network on an open LAN.[2] Agent presence checking, hardware-asset tracking, and remote configuration are available even when a PC is awake, working properly, and connected to the corporate network through a host OS-based VPN.

PC-initiated communications can be requested from in-band or out-of-band (OOB). In-band, a communications agent passes the request to the hardware and firmware. After that, secure communications are established through the TLS-secured OOB communications channel to the IT console. OOB communications can be established either by the PC itself (requesting service or passing a critical alert) or established by the user by interrupting the boot process at BIOS with a command key or hotkey which then connects the PC to the IT console for service.

PC-initiated communications can be particularly useful for:

- Out-of-band remote diagnostics and repair. Since the PC can initiate secure communications even if the OS is down, users can get faster service without having to make a service-depot call.
- Remote scheduled system maintenance, including patching, system defense filter updates, audits/event logs, and inventory reporting.
- Alerting, so IT technicians can be quickly notified when a problem occurs – such as a notebook falling out of compliance, or hard disk filling to capacity – so they can proactively maintain and service PCs before an OS or application becomes inoperable.

Capabilities to meet your critical use cases

Intel vPro technology is designed to help IT administrators reach more PCs remotely, automate more tasks, and perform more work from a remote, centralized location. This can help business reduce user interruptions, improve work flow, and reduce the total cost of owning technology.

Tables 1 through 5 list common use cases for improved communication, security, maintenance, and management, along with the capabilities that enable them. Remote configuration options are described later in this white paper, on page 25.

Table 1. Communication capabilities

Capability	What it does	Common uses
Secure tunnel for out-of-band communication	Allows an IT console to communicate securely with a notebook or desktop PC virtually anytime.	• Remotely and securely communicate with the PC, even if PC power is off, the OS is unresponsive, management agents are missing, or hardware (such as a hard drive) has failed.
Secure tunnel for communication outside corporate firewall[2]	Allows a notebook or desktop PC to initiate secure communications with a remote management console through a TLS-secured tunnel for updates, diagnostics, repair, alert reporting, and other tasks.	• Remotely and securely service PCs at satellite offices, outside the corporate firewall, in locations that don't have an onsite proxy server or management appliance, such as at a small business client's remote location. • Hotkey feature for users to quickly and securely connect the PC to the IT console for service. • OOB PC-initiated request for prescheduled maintenance over secure communication tunnel. • OOB PC-initiated alert sent over secure communication tunnel back to IT console.

Table 2. Power-management capability

Capability	What it does	Common uses
Remote power up/down/reset	Securely and remotely power up, power down, or power cycle a PC.	• Power up PCs off-hours for updates and patches, even for PCs that don't have agents installed. • Mass shut-down during malicious attacks. • Power-manage the PC to reduce power consumption when the PC is not in use and save on energy costs.

Table 3. Security capability

Capability	What it does	Common uses
Agent presence checking	Third-party applications check in with hardware-based timers at IT-defined intervals. A "miss" triggers an event and can send an alert to the IT console to indicate potential problems.	• Automated, out-of-band notification of a missing or disabled agent (in combination with policy-based out-of-band alerting).
System isolation and recovery	Programmable filters check inbound and outbound network traffic for threats before the OS and applications load and after they close down.	• Monitor inbound/outbound network traffic for threats. • Identify suspicious packet headers. • Identify suspicious packet behavior, including fast-moving and slow-moving worms (desktop PCs with Intel® vPro™ technology). • Port-isolate or quarantine PCs even if agent or OS is disabled.
Intel® Anti-Theft Technology for notebooks[3]	Gives IT administrators the option of disabling the PC and/or protecting encrypted data from unauthorized access if a notebook is lost or stolen.	• Use programmable triggers and poison-pill responses to identify and prevent unauthorized access to a notebook's encrypted data, and/or disable the PC if the system is lost or stolen.
Support for 802.1x, Cisco SDN,* Microsoft NAP,* and PXE (preexecution environment)	Lets the network verify a PC's security "posture" even before the OS loads before allowing the PC access to the network.	• Enable remote, out-of-band management and PXE boot of the PC while still maintaining full network security in a Cisco SDN or Microsoft NAP environment.
Access to critical system information[a]	Lets you access critical system information (such as software version information, .DAT file information, and machine IDs) anytime.	• Verify a PC's posture. • Identify PCs that need to be updated or patched, even for PCs that do not have an agent installed.

[a] Access to dedicated, protected memory, including UUID, event logs, hardware asset information, and software asset information in the third-party data store is also available when the PC is connected to the corporate network through a host OS-based VPN.

Table 4. Problem-resolution capability

Capability	What it does	Common uses
Remote/redirected boot	More securely remote boot PC to a clean state, or redirect the PC's boot to another device, such as a clean image on local storage, a CD at the help desk, or an image on another remote drive.	▪ Remotely boot PC to clean state. ▪ Remotely boot PC to remediation server. ▪ Remotely watch as BIOS, OS, and drivers load to identify problems with boot process. ▪ Remotely provision PC before agents are installed. ▪ Remotely rebuild or migrate OS. ▪ Remote BIOS updates.
Console redirection	Secure console redirection to remotely control a PC without user participation.	▪ Troubleshoot PC without user participation. ▪ Remotely install missing/corrupted files. ▪ Remote hard-drive service or other maintenance.
Out-of-band alerting	Receive policy-based alerts anytime – securely – from inside or outside the corporate firewall, even if the OS is unresponsive, management agents are missing, or hardware (such as a hard drive) has failed.	▪ Alert on event, such as falling out of compliance (in combination with agent presence checking). ▪ Alert on thresholds, before component fails. ▪ Receive alerts from outside the corporate firewall via PC-initiated secure communications.[2]
Hotkey fast-connect to the IT console[2]	Users can use a hotkey combination to initiate a secure connection to the IT console for help or for PC servicing, from inside or outside the corporate firewall.	▪ PC-initiated, secure remote connection to IT console.
Persistent event logs[a]	Event log stored in persistent, dedicated memory (not on the hard drive), available anytime.	▪ Access list of events that occurred before a hardware or software problem was noticed, including events that occurred before a notebook connected to the network. ▪ Confirm critical events. ▪ Auditor oversight of the event log, as well as view and erase.
Access to BIOS settings	Allows access to BIOS settings anytime.	▪ Remotely correct BIOS settings accidentally changed by user. ▪ Remotely change BIOS settings to solve application conflicts. ▪ Remotely change PC's primary boot device to meet user needs.
Access to critical system information[a]	Lets you access critical hardware asset information (such as manufacturer and model number) anytime, even if hardware (such as a hard drive) has already failed.	▪ Identify "missing" (failed) hardware components.

[a] Access to dedicated, protected memory, including UUID, event logs, hardware asset information, and software asset information in the third-party data store is also available when the PC is connected to the corporate network through a host OS-based VPN.

Table 5. Asset-management capability

Capability	What it does	Common uses
Persistent universal unique identifier (UUID)[a]	Lets you identify PC anytime, even if PC power is off, the OS has been rebuilt, hardware or software configuration has changed, or the hard drive has been reimaged.	▪ Accurately discover and identify PCs on network. ▪ Identify unauthorized devices on the network.
Access to hardware asset information[a]	Access hardware asset information (such as manufacturer and model number) anytime.	▪ Accurate remote hardware-asset inventory. ▪ End-of-lease planning. ▪ FRU inventory management. ▪ Identify upgrade opportunities.
Access to third-party data storage[b]	Store and access critical software asset information (such as version information) in dedicated, persistent memory.	▪ Remote software-asset inventory[b]. ▪ Software license planning.

[a] Access to dedicated, protected memory, including UUID, event logs, hardware asset information, and software asset information in the third-party data store is also available when the PC is connected to the corporate network through a host OS-based VPN.

[b] You can perform a remote software-asset inventory by accessing software information stored in the third-party data store; or by powering up an AC-powered, wired PC, and then performing the remote software inventory through the software inventory agent.

Use an existing management console for both notebook and desktop PCs

Notebook and desktop PCs with Intel vPro technology use the same management console and communication mechanisms as other PCs. You can manage both notebook and desktop PCs with Intel vPro technology from the same IT console.

Leading management software companies such as HP, LANDesk, Microsoft, and Symantec have optimized their software to take advantage of the advanced capabilities of Intel vPro technology. These vendors support both previous and current versions of Intel vPro technology. IT administrators who have already deployed PCs with Intel vPro technology do not have to change their management console to use PCs with the current version of Intel vPro technology. Ask your management-console vendor about specific implementation schedules and support for the new hardware-based security and remote-management capabilities for both notebook and desktop PCs.

Managing wired or wireless PCs

PCs with Intel vPro technology are designed to keep your workforce mobile, managed, and secure, whether working on a notebook or desktop PC. They are also designed to make management easier for both wired and wireless states:

- Identify notebook or desktop PC power state remotely.
- Maintain and manage the notebook in both wired and wireless states.
- Communicate more securely with notebook or desktop PCs in an open wired LAN — even outside the corporate firewall.
- Protect a notebook's data and its OS even if the system is lost or stolen.
- Secure, manage, and maintain PCs remotely — without user participation.

Manage PCs regardless of power state

PCs with Intel vPro technology are designed to give IT technicians greater remote visibility into the system in both wired and wireless states, as described in Table 6. Technicians can remotely power up a wired or wireless notebook or wired desktop PC almost anytime. (In order to prevent unexpected battery use in notebooks, remote power-up is not applicable to the battery-powered, wireless sleep state). Technicians can also reboot the PC, use secure console redirection, and use other critical maintenance and management capabilities of Intel vPro technology for wired or wireless PCs.

With the ability to remotely wake, power up, maintain, and manage a PC anytime, technicians can ensure that IT tasks are performed when needed for security, and also performed at advantageous times for mobile users — without requiring user participation.

Table 6 shows how the capabilities are enabled for wired and wireless notebooks and for wired desktop PCs, both inside and outside the corporate network.

Improved power-management and energy efficiency

Notebooks with Intel vPro technology are designed to help conserve energy so users can stay unplugged with the longest possible battery life. For example, these systems include a power-optimized chipset, ultra-low wattage electronics, and a new sleep state (C6) which allows the system to power down one processor core when it is not needed.

Intel Centrino 2 with vPro technology-based notebooks deliver:

- Variety of power-management options to extend battery life.
- Integrated energy-saving components that are optimized to extend battery life.
- DDR3 memory, which reduces total device power, but still allows data to flow faster.
- Energy Star* Ready.

Secured out-of-band PC management

Software-only management applications are usually installed at the same level as the OS. This leaves their management agents vulnerable to tampering. Communication privacy is also an issue in today's PCs because the in-band, software-based communication channel they use is not secure.

In contrast, Intel vPro technology delivers both "readily-available" (out-of-band) remote communication built into the PC, as well as robust security technologies. These security technologies help ensure that the powerful capabilities of Intel vPro technology, as well as your stored information, are better protected.

Remote-communication channel runs outside the OS

The communication channel used by Intel vPro technology runs outside the OS (see figures 2 and 3). This OOB channel is based on the TCP/IP firmware stack designed into system hardware, not on the software stack in the OS. The channel allows critical system communication (such as alerting) and operations (such as agent presence checking, remote booting, and console redirection) to continue more securely virtually anytime.

Table 6. Capability matrix for notebooks and desktop PCs

Use Cases	Usages	Works with wired PC-initiated secure communication outside corporate firewall[a]	AC-powered wired or wireless notebook or wired desktop			Battery-powered wired or wireless notebook		
			Awake, OS working properly	Awake, but OS unresponsive	Asleep (Sx)	Awake, OS working properly	Awake, but OS unresponsive	Asleep (Sx)
Remote power up/power cycle	IT resets PC to clean state (or powers up PC for servicing). Use power management to reduce energy costs.	Yes	Yes	Yes[b]	Yes	Yes	Yes[b]	N/A
Encrypted, remote software update	Automated or manual policy-based protection against virus outbreaks.	Yes	Yes	Yes[b]	Yes	Yes	Yes[b]	N/A
Agent presence checking and alerting	Ensure critical applications are running, and be quickly notified when they miss a check in.	Yes	Yes Also available when using host OS-based VPN	Yes[b]	N/A	Yes Also available when using host OS-based VPN	Yes[b]	N/A
System isolation and recovery	Automated or manual policy-based protection against virus outbreaks.	Yes	Yes	Yes[b]	N/A	Yes	Yes[b]	N/A
Protection for data if a notebook is lost or stolen	Identify and prevent unauthorized access to encrypted data, or disable the notebook if it is lost or stolen.	N/A	Yes for notebooks Also available when using host OS-based VPN	Yes for notebooks	N/A	Yes Also available when using host OS-based VPN	Yes	N/A
Remote diagnosis and repair	Diagnose and repair problems remotely via out-of-band event log, remote/redirected boot, console redirection, and preboot access to BIOS settings.	Yes	Yes	Yes[b]	Yes	Yes	Yes[b]	N/A
Remote hardware and/or software asset tracking	Take a hardware or software inventory regardless of OS state or power state.	Yes	Yes Also available when using host OS-based VPN	Yes[b]	Yes	Yes Also available when using host OS-based VPN	Yes[b]	N/A
Remote configuration	Configure and provision PCs securely without a deskside visit.	N/A	Yes	N/A	N/A	Yes	N/A	N/A

[a] Systems using client-initiated remote access require wired LAN connectivity and might not be available in public hot spots for "click to accept" locations. For more information on PC-initiated remote access, visit, www.intel.com/products/centrino2/vpro/index.htm. PC-initiated remote communication is supported only in the latest notebooks and desktop PCs with Intel vPro technology.

[b] Requires WPA or WPA2/802.11i security and Controller Link 1 for wireless operation when user OS is down.

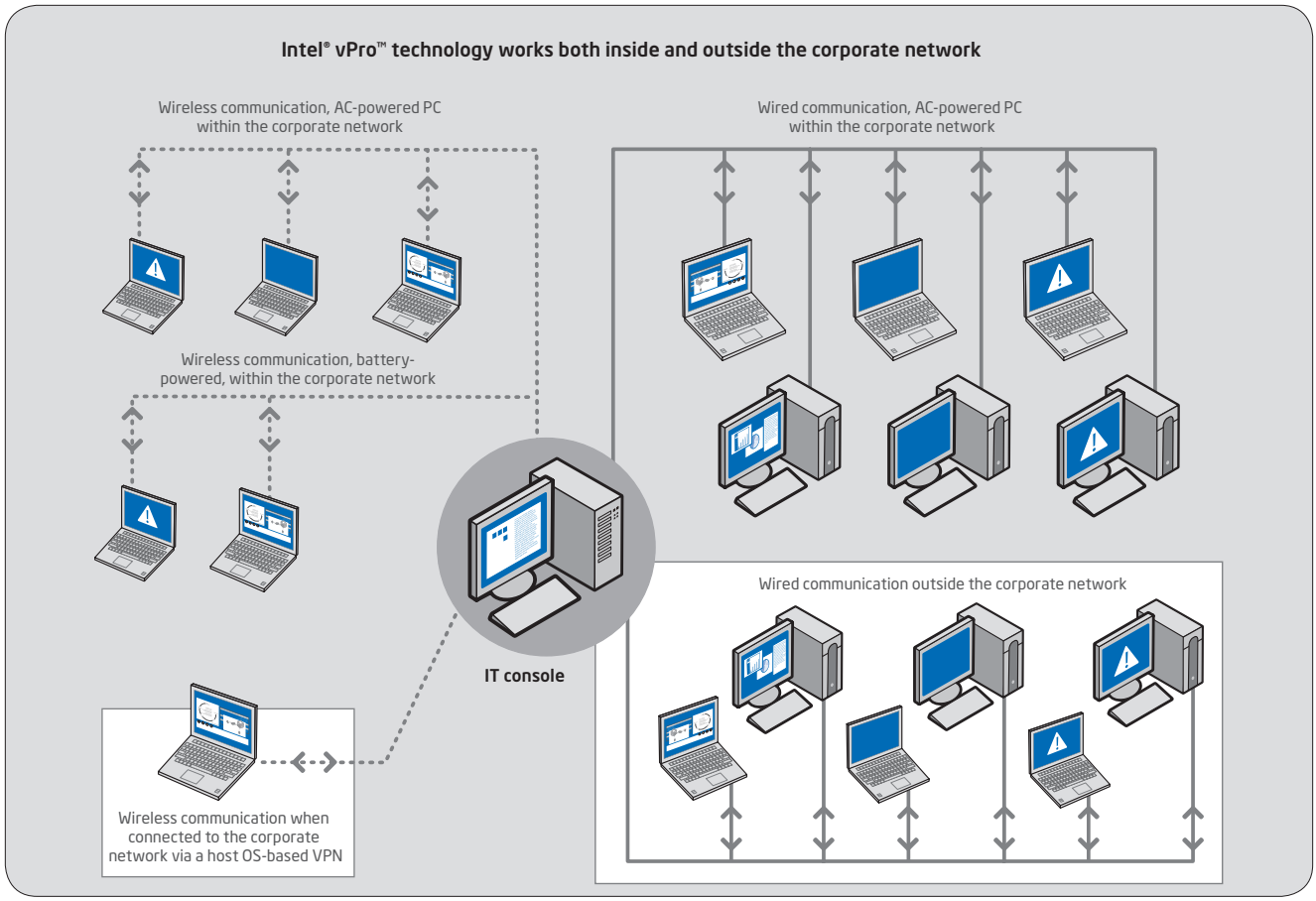

Figure 2. Remote communication. Capabilities are available for both wired or wireless notebooks and wired desktop PCs with Intel® vPro™ technology inside the corporate firewall. All capabilities are also available for wired PCs outside the corporate network on an open LAN.[2] Some remote service capabilities for wireless notebooks with Intel vPro technology are also available when the notebook is connected to the corporate network through a host OS-based VPN.

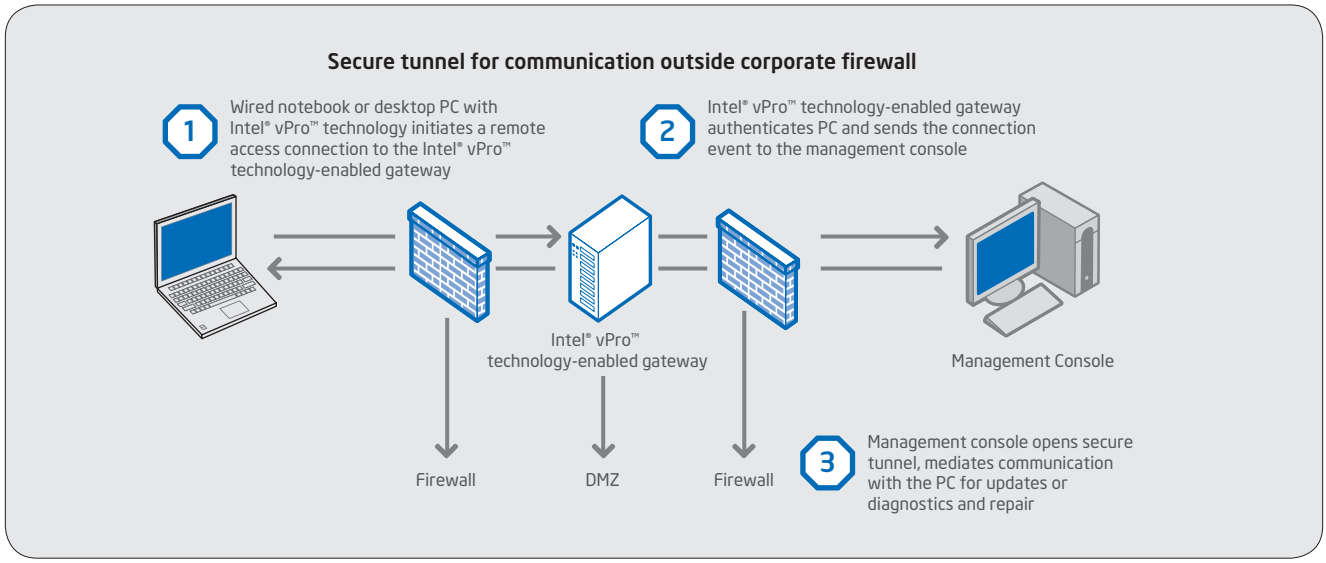

Figure 3. More secure communication to wired PCs outside the corporate firewall. An Intel® vPro™ technology-enabled gateway authenticates wired PCs, opens a secure TLS tunnel between the management console and PC, and mediates communication.

Because the channel is independent of the state of the OS, authorized IT technicians can communicate with PCs:

- **Wired AC-powered PC —** anytime. Even if hardware (such as a hard drive) has failed, the OS is unresponsive, the PC is powered off, or its management agents are missing,[1] the communication channel is still available. As long as the system is plugged into a wired LAN and connected to an AC power source, the channel is available to authorized technicians.
- **Wireless notebook on battery power —** anytime the system is awake and connected to the corporate network, even if the OS is unresponsive.[14]
- **Wired, connected to the corporate network over a host OS-based VPN —** anytime the system is awake and working properly.

More secure wired communication outside the corporate firewall

Notebooks and desktop PCs with Intel vPro technology support secure communication in an open wired LAN – outside the corporate firewall.[2] This capability allows a wired PC to initiate communication with a remote management console through a secured tunnel for inventories, diagnostics, repair, updates, and alert reporting. IT managers now have critical maintenance and management capabilities for wired PCs in satellite offices, outside the corporate firewall, and in locations that don't have an onsite proxy server or management appliance, such as at a small business client's remote location:

- Securely update and service wired PCs, via a prescheduled maintenance time when the PC initiates a secure connection to the IT console. This capability is available even when the system is outside the corporate firewall.
- Remote IT alert, so the wired PC can initiate a secure connection to the IT console to automatically send an alert from agent presence checking, system defense triggers, or other critical events.
- Hotkey auto-connection to IT console, so a user can quickly connect the wired PC to the IT console for help or system servicing.

The PC-initiated communications capability works through the use of an Intel vPro technology-enabled gateway in the DMZ (demilitarized zone) that exists between the corporate and client firewalls. System configuration information in the wired PC includes the name(s) of appropriate management servers for the company. The gateway uses that information to help authenticate the wired PC. The gateway then mediates communication between the PC and the company's management servers during the repair or update session (see Figure 3).

Operate wirelessly with greater link reliability and predictability

Notebooks with Intel® Centrino® 2 with vPro™ technology support wireless technologies, including:

- 802.11a/b/g protocols for more secure, flexible wireless connectivity.[7]
- 802.11n, the new standard expected to deliver up to 5x improvement in data throughput on a wireless-n network.[16]
- Current Cisco*-compatible extensions and features for improved network performance and Voice over WLAN, by optimal access-point selection technology.
- Optional, integrated WiFi/WiMAX – with WiFi performance of up to 450 Mbps – for metro-wide broadband connectivity, so users can be ready for on-the-go wireless access beyond today's hot spots.[4]

802.11n delivering performance gains of up to 5x.

Notebooks with Intel® vPro™ technology and Intel® Next-Gen Wireless-N[17] on a new wireless 802.11n network deliver better reliability by reducing dead spots and dropped connections to improve productivity with fewer wireless interruptions. These notebooks also provide improved wireless connectivity for mobile users at the office. Among its many benefits, Intel Next-Gen Wireless-N technology can deliver up to five times the performance of existing 802.11g networks,[16] with faster and more reliable wireless coverage.

Intel is committed to the adoption of the 802.11n standard. Intel has worked closely with leading wireless Access-Point (AP) vendors and has conducted extensive testing to verify the implementation of the technology. IT administrators can be assured that notebooks with Intel vPro technology and Intel Next-Gen Wireless-N work well with existing 802.11a/b/g access points and also provide great benefits with new wireless-n networks.

PC-initiated secure communication

PC-initiated secure communication is a collaborative effort in the industry. Intel is working closely with leading independent software vendors (ISVs) to enable this critical capability in management consoles and firewalls.

Robust security methodologies for communication

The hardware-based communication and manageability capabilities are secured through a variety of robust schemes. These include:

- Transport Layer Security (TLS).
- HTTP authentication.
- Enterprise-level authentication using Microsoft Active Directory* (Kerberos).
- Access control lists (ACLs).
- Digital firmware signing.
- Other advanced methodologies and technologies.

The security measures built into notebook and desktop PCs with Intel vPro technology can be active even when the PC is off, software agents have been disabled, or the OS is unresponsive. These measures help ensure the security of stored information and the confidentiality and authentication of the communication channel and hardware-based capabilities.

PCs with Intel vPro technology also include built-in security capabilities to help protect themselves (refer to the next discussion).

Best for business: Defense in depth

IT administrators typically identify their most critical challenge as securing PCs from malicious attacks. The traditional problem is that even the best software-only solution can't manage systems that are powered off or whose OS is unavailable.

The proven hardware-based security capabilities of Intel vPro technology combine with new capabilities to deliver proactive protection that helps the PC itself guard your business from data loss and interruptions:

- Eliminate virtually all deskside visits traditionally required to update or patch PCs.[15]
- Remotely power on PCs for off-hours updates, patching, or other work, even if the system is outside the corporate firewall.
- Remotely identify PCs that are out of compliance.
- Rely on programmable, automated hardware-based filters to check network traffic even when PCs are in the traditionally vulnerable state before the OS and applications load, and after they shut down.
- Use programmable, automated hardware-based triggers in notebooks to identify unauthorized attempts to access data or the OS, and lock out the unauthorized user with the appropriate poison-pill response.

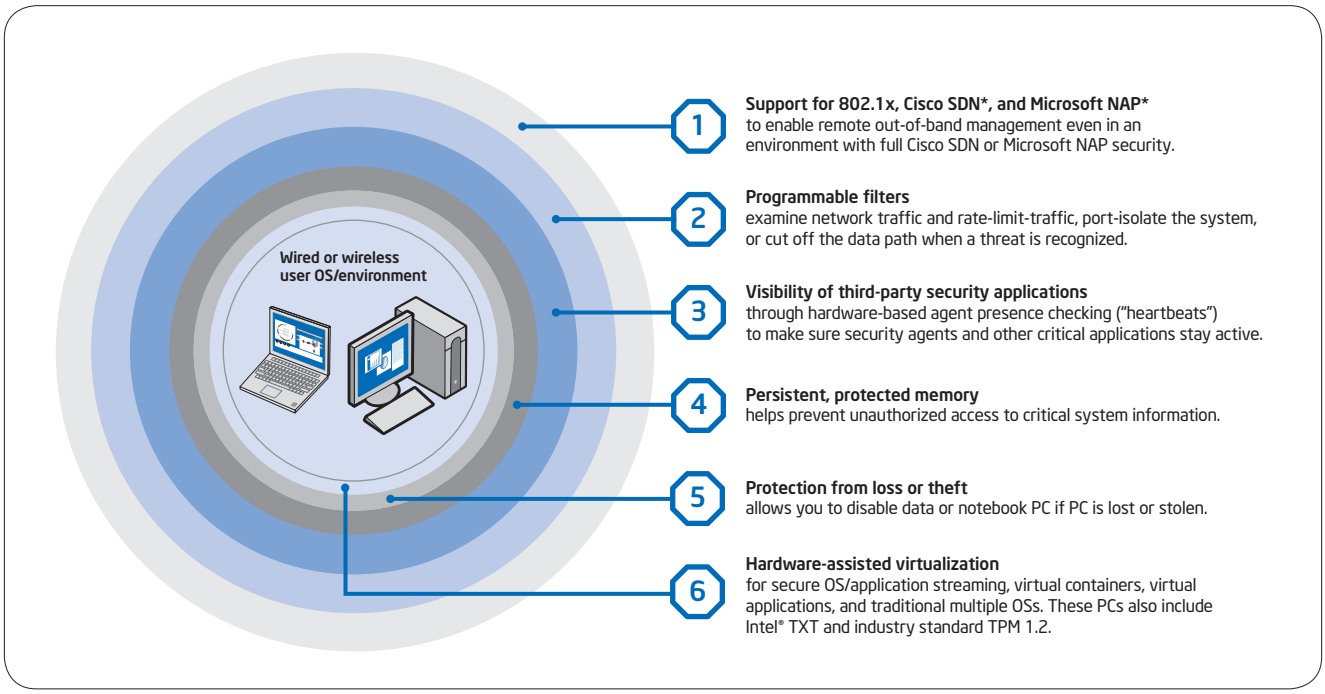

Figure 4. New layers of defense. Hardware-based security capabilities offer new layers of defense to fortify the PC against critical threats.

New layers of defense

Notebook and desktop PCs have several distinct layers of hardware-based protection:

- Programmable filtering of inbound and outbound network traffic, and out-of-band isolation capabilities.
- Remote visibility of software agents.
- Optional Intel Anti-Theft Technology (Intel AT) for notebooks.
- Dedicated memory to better protect critical system information from viruses, worms, and other threats.
- Out-of-band management even in 802.1x, PXE, Cisco SDN, and Microsoft NAP environments.
- Intel® Trusted Execution Technology (Intel® TXT).
- Industry-standard TPM 1.2.
- Hardware-assisted virtualization for next-generation delivery models of OS and applications into secure virtual environments, as well as hardware-assisted traditional virtualization.

These new layers of defense make it easier to identify threats faster on both wired and wireless systems, and stop them more effectively before they begin to spread.

Intel® Anti-Theft Technology (Intel® AT)

Businesses face two increasingly daunting challenges in managing and securing mobile PCs: increasing numbers of data breaches, identity theft, and computer theft, and compliance with increasingly stringent regulations in data security and privacy. Notebooks with Intel vPro technology addresses these challenges by building important new optional security technology, called Intel Anti-Theft Technology (Intel AT) into notebook hardware.[3] Intel AT delivers client-side intelligence that protects encrypted data and system configurations against unauthorized access if a notebook is lost or stolen.

"Poison-pill" response to disable PC or lock out access to data

Intel AT uses a set of programmable and interdependent hardware-based triggers and responses to identify unauthorized attempts to access encrypted data or the OS. Triggers include repeated login failures, failure to log into a central server within a particular timeframe, or a receipt of a notice from the central server to disable the PC or data access. Poison pill responses can be:

- Local and self-administered, based on a trigger, so that the notebook has local, self-initiated defense, even when it is disconnected from the network.
- Remote and administered by IT, based on an alert or upon receiving a call from the user (for example, that the notebook was lost while traveling).

IT can use flexible policies to specify that the poison pill:

- Disable access to encrypted data by deleting software-based encryption keys or other cryptographic credentials required for access to data.
- Disable the PC, so it cannot boot the OS, even if the hard drive is replaced or reformatted.
- Disable both the PC and access to encrypted data.

For example, IT could define a trigger so that the system locks down after five attempts to log in. IT could also define a trigger for critical machines, such as a financial officer's notebook, so that, if the system does not connect to the central server every day, access to the system is disabled. If the notebook is reported lost, an IT administrator can flag the system in a central database. The next time the notebook connects to the Internet, it calls home using in-band communication and synchronizes with the central server. When Intel AT receives the server's notification that the notebook has been flagged as lost or stolen, Intel AT disables the PC and/or access to data, according to IT policy.

Easy reactivation and full system recovery

Intel AT includes two reactivation mechanisms:

- Local pass-phrase, which is a strong password preprovisioned in the notebook by the user. The user enters this passphrase in a special pre-OS login screen in order to reactivate the system.
- Recovery token, which is generated by IT or the user's service provider via the theft management console (upon request by the end user). The one-time recovery token is provided to the user via phone or other means. The user then enters the token in a special pre-OS login screen in order to reactivate the system.

Both methods return the PC to full functionality, and both offer a simple, inexpensive way to recover the notebook without compromising sensitive data or the system's security features.

Industry support and software development

Major OEMs and ISVs are working closely with other industry players to implement this critical new security technology. OEMs who offer notebooks that support Intel AT include Lenovo and Fujitsu Siemens Computers.

Intel AT integrates with existing theft-management solutions. ISVs who support Intel AT include Absolute Software Corporation and Phoenix Technologies Ltd., and additional security ISVs are planning to offer solutions in 2009.

In order to deploy an Intel AT solution, a service provider or ISV with Intel AT capabilities is required. Intel vPro technology includes an SDK and documentation for ISVs and service providers to help test and validate their designs for Intel-AT-capable products.

Intel AT does not rely on the presence or activation of a TPM. You do not need TPM in order to take advantage of Intel AT.

Intel AT is also independent of Intel Active Management Technology (Intel AMT). You do not need to enable Intel AMT in order to take advantage of Intel AT.

Push updates down the wire — regardless of PC power state

There are several methods in use today to wake a PC in order to push out an update, but those methods are not secure, or they work only when the OS is running properly. In contrast, Intel vPro technology includes a secure, encrypted power-up capability that helps technicians ready systems for updates. This helps IT organizations substantially speed up and ensure greater saturation for critical updates and patches. With Intel vPro technology, technicians can:

- Remotely power up notebook and desktop PCs from the IT console, so updates can be pushed even to machines that were powered off at the start of the maintenance cycle.
- Deploy more updates and critical patches off-hours or when it won't interrupt the user.
- Check a PC's software version information, .DAT file information, and other data stored in nonvolatile memory, and find out if anything needs updating without waking up a PC.
- Help lower power consumption for businesses, by powering PCs off when not in use, and remotely and securely powering them up off-hours only for the update or patch (or other service).

These capabilities allow IT administrators to automate more security processes. In turn, this can help IT administrators establish a more secure, better managed environment.

Greater automation for compliance with corporate policies

With the ability to remotely access PCs, IT administrators can automate more processes, including update, remediation, and management processes. For example, if a polling agent discovers software that is out of date, the third-party management application can automatically take a software inventory, port-isolate the system temporarily, and then update the system. The management application can then remotely return the system to its previous power state: on, off, hibernating, or sleeping. This can help administrators eliminate many of the traditional deskside visits and service depot calls required for updates, critical patches, and remediation, and help reduce risks to the network.

Filter threats and isolate PCs automatically based on IT policy

Notebook and desktop PCs with Intel vPro technology include programmable filters that monitor inbound and outbound network traffic for threats. With Intel vPro technology, IT managers can use third-party software to define the policies that will trigger hardware-based isolation of a PC.

Both notebooks and desktop PCs with Intel vPro technology use programmable, hardware-based filters for examining packet headers for suspicious behavior. Desktop PCs with Intel vPro technology also include additional hardware-based filters that monitor the rate of outbound traffic to help identify suspicious behavior, including both fast-moving and slow-moving worms.

Both notebook and desktop PCs also include built-in isolation circuitry (see Figure 5). When a threat is identified, a policy and hardware-based "switch" can:

- Isolate the system by specific port(s) to halt a suspicious type of traffic.
- Disconnect the network data path to the OS (the remediation port remains open) to contain threats more quickly.
- Rate-limit network traffic to give a technician more time to investigate a threat.

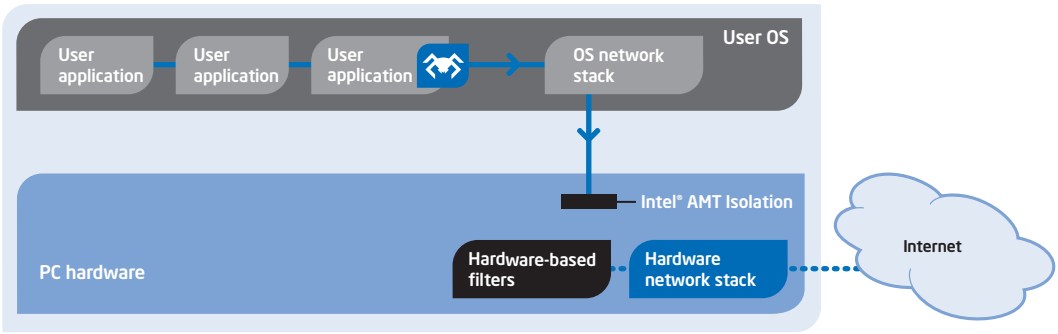

Figure 5. System defense filters inspect network traffic. A PC with Intel® vPro™ technology can port-isolate itself or cut off its own network data path to quarantine itself when suspicious behavior is recognized even if its OS is not available to help prevent threats from spreading to the network

During a quarantine, the isolation circuitry disconnects the PC's network communication via hardware/firmware at the software stack in the OS. This is a more secure disconnect than traditional software-based isolation, which can be circumvented by hackers, viruses, worms, and user tampering.

Automated, continual checking for agents

Traditionally, IT organizations have used serial polling to verify the presence of security agents (or other business-critical applications). Because this method can saturate the network with healthy heartbeats (restricting the bandwidth available for productive traffic), IT organizations often poll for compliance only once or twice a day if that often.

In contrast, notebook and desktop PCs with Intel vPro technology use a regular, programmable "heartbeat" presence check, which is built into the Intel® Management Engine. The heartbeat uses a "watchdog" timer so third-party software can check in with the Intel Management Engine at programmable intervals, to confirm that the agent is still active. Each time an agent checks in, it resets its timer. If an agent hasn't checked in before the timer goes off, the agent is presumed removed, tampered with, or disabled. The Intel Management Engine then automatically and immediately logs the alert and notifies (if specified) the IT console.

With hardware-based heartbeats, IT administrators no longer need to wait for multiple polls to identify a potential problem. The PC itself helps improve the reliability of presence checks and reduce the window of software vulnerability. And, these "healthy" heartbeats never leave the PC. Only when there is a problem is data sent across the network, so your network isn't flooded with healthy heartbeat signals, and you still receive rapid notification of problems.

For wireless notebooks, agent presence checking is enabled even when operating outside the corporate network through a host OS-based VPN. This gives IT administrators greater visibility of these highly mobile and traditionally unsecured assets.

Combined with the remote power-up capability, the entire process of checking and reinstalling missing agents can also be automated, improving compliance further and saving additional resources.

Receive alerts even if a system is off the corporate network

Notebook and desktop PCs with Intel vPro technology have policy-based alerting built into the system. IT administrators can define the types of alerts they want to receive. Although all alerts are logged in the persistent event log, IT administrators can receive only the alerts they want. In this way, alerts that are not as critical do not add substantially to network traffic.

Alerting within the corporate network

Since alerting uses the OOB communication channel, IT administrators can receive critical notifications from PCs within the corporate network out-of-band, virtually anytime, even if the OS is inoperable, hardware has failed, or management agents are missing.

Alerting from outside the corporate network

IT can even receive notifications from a PC (awake and OS operable) that is connected to the corporate network through a host OS-based VPN or when connected via wired LAN on an open network outside the corporate firewall. Because PCs with Intel vPro technology can initiate a secure communications tunnel to the IT console, these PCs can also send an alert (defined by IT policy) from outside the corporate firewall.

IT administrators can now be notified rapidly and automatically virtually anytime a system falls out of compliance, or hardware is about to fail – sometimes even before users know they have a problem, or applications hang.

Out-of-band management even with 802.1x, Cisco SDN, and Microsoft NAP

In the past, IT administrators often felt they had to choose between using out-of-band management and maintaining full network security with 802.1x, Cisco SDN, or Microsoft NAP. With the latest PCs with Intel vPro technology, network security credentials can be embedded in the hardware. This includes an Intel® Active Management Technology[1] (Intel® AMT) posture plug-in, which collects security posture information (such as firmware configuration and security parameters), and the Intel AMT Embedded Trust Agent.

This capability allows the 802.1x authentication or the Cisco, or Microsoft posture profile to be stored in hardware (in protected, persistent memory), and presented to the network even if the OS is absent. The network can now authenticate a PC before the OS and applications load, and before the PC is allowed to access the network. IT administrators can now use out-of-band management for maintenance, security, management, or PXE purposes, while still maintaining full network security, including detailed, out-of-band compliance checks.

This capability also allows IT administrators to use their existing PXE infrastructure within an 802.1x, Cisco SDN, or Microsoft NAP network. The result is better security for PCs and a more reliable network, regardless of the PC's OS state, application state, or the presence of management agents.

Intel® Trusted Execution Technology (Intel® TXT)

The new generation of notebook and desktop PCs with Intel vPro technology include Intel TXT, as well as industry-standard TPM 1.2. Intel TXT helps build and maintain a chain of trust from hardware to an Intel TXT-enabled OS or application. For example, Intel TXT can build and maintain a chain of trust from hardware to a Virtual Machine Monitor (VMM) to protect information in virtualized environments from software-based attacks.

PCs with Intel vPro technology also include industry standard TPM 1.2, which stores keys in hardware, so security measures such as hard-drive encryption (for example, via Windows BitLocker full drive encryption) are more effective. TPM 1.2 is compatible with both Windows Vista TPM driver and TPM base service.

Substantially improve efficiencies for remote maintenance and management

Intel vPro technology provides many innovative and hardware-based capabilities already proven to significantly improve maintenance and management tasks, such as discovery, inventory, daily maintenance, updates, and problem resolution. These capabilities are available to authorized technicians virtually anytime.

Studies show that the new capabilities can help IT organizations reduce the number of deskside visits or service depot calls traditionally required to inventory, upgrade, repair, rebuild, or reimage PCs by up to 56%.[18]

With better remote tools, IT administrators can also automate more of these tasks. And, with greater visibility and access to the PC's state, more work can be performed off-hours or when it is otherwise convenient to users.

Table 7. Intel® vPro™ technology reduces deskside visits[18]

Issue	Estimated improvement with Intel® vPro™ technology[18]
Hardware problems for notebook and desktop PCs	Reduce service depot and deskside visits by up to 56%
Software problems for notebook and desktop PCs	Reduce service depot and deskside visits by up to 58%

Resolve more problems remotely

One of the most critical IT needs is a greater ability to remotely resolve PC problems, especially for mobile PCs, and especially when a system's OS is down or hardware has failed. According to industry studies, deskside and service-center calls make up only a small percent of PC problems in a typical business, but they take up the majority of the budget. In fact, the cost of a deskside visit is seven times the cost of a remote problem resolution.

Problem-resolution capabilities in Intel vPro technology include:

- **Remote/redirected boot**, through integrated drive electronics redirect (IDE-R), a more powerful and secure capability than wake-on-LAN (WOL). IDE-R allows authorized IT technicians to remotely boot a PC to a clean state, or redirect the boot device for a problem PC to a clean image on local storage, on a CD at the help desk, or to an image on another remote drive. There is no need for a deskside visit or service depot call to resolve many boot, OS, and software remediation problems.
- **Console redirection**, through Serial-Over-LAN (SOL). Technicians now have remote keyboard and video console control of a PC outside of standard OS control, allowing them to perform tasks such as editing BIOS settings from the service center – without user participation.
- **Out-of-band**, policy-based alerting, so the PC can send alerts and Simple Network Management Protocol (SNMP) traps to the management console anytime, based on IT policies.
- **Persistent event logs**, stored in dedicated memory (not on the hard drive) so the information is available anytime. IT technicians can now access the list of events that occurred even before a hardware or software problem was noticed, including events that occurred before a PC connected to the network.
- **Always-available asset information**, stored in dedicated, protected memory. This information is updated every time the system goes through power-on self test (POST).
- **Access to preboot BIOS** configuration information anytime.

Diagnostics and repair processes can also be securely performed on wired PCs – even outside the corporate firewall.[2]

Using the diagnostics and repair capabilities of Intel vPro technology, IT administrators can substantially reduce deskside visits (see Table 7), improve mean time to repair, reduce user downtime, and improve technician efficiencies.

IT technicians can now remotely:

- Access asset information anytime, to identify "missing" or failed hardware components, and verify software version information.
- Guide a PC through a troubleshooting session without requiring user participation.

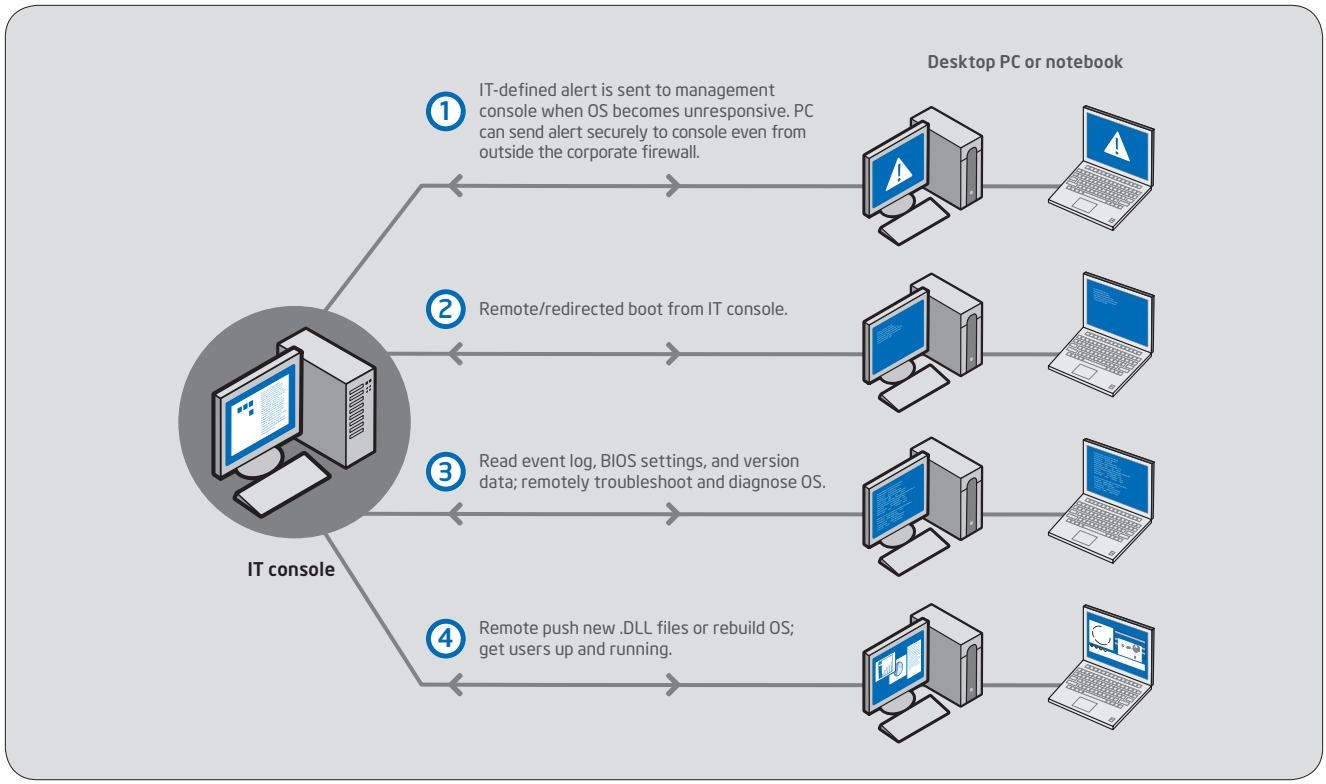

Figure 6. Remote problem resolution for an inoperable OS. The capabilities allow a technician to remotely access, diagnose, and repair or rebuild an OS that has become inoperable.

- Reboot a system to a clean state, or redirect the PC's boot device to a diagnostics or remediation server (or other device).
- Watch as BIOS, drivers, and the OS attempt to load, to identify problems with the boot process.
- Update BIOS settings, identify BIOS versions, or push a new BIOS version to the PC to resolve a particular problem.
- Upload the persistent event log to identify the sequence of events (such as temperature spikes or an unauthorized software download) that occurred before the system failed.
- Push new copies of missing or corrupted files, such as .DLL files, to restore an OS.
- Rebuild the OS or fully reimage the hard drive remotely.
- Perform OS migrations and application upgrades.
- Power-manage PCs more effectively to lower power consumption and reduce energy costs.

If a system becomes inoperable (see Figure 6), a technician can use secure remote/redirected boot or a secure PXE boot to change the system's boot device to a CD or to an image located on a remote network drive – without leaving the service center. The technician can then use secure console redirection to remotely guide the PC through a troubleshooting session. If a user application has become corrupted, the technician can remotely reimage the user's hard drive and restore user data from known-good files, overwriting corrupt or problem files. The user is back up and running as quickly and efficiently as possible without a service depot call or deskside visit.

Many case studies have shown how Intel vPro technology can help substantially reduce IT service costs for problem resolution (refer to the Intel Web site for case studies in various industries[20]) and software updates, including patching. For example, the Government of the State of Indiana recently reported that using Intel vPro technology to improve remote management has reduced deskside visits by 80%, expects savings of over $172,000 in the first year alone, and projects a break-even point in just over one year and a positive ROI of 472% over four years.[21]

Accurate, remote discovery and inventory for wired or wireless systems

One of the primary challenges in managing PCs is acquiring information that is typically lost or unavailable when a system is powered down, reconfigured, rebuilt, or inoperative.

On average, up to 20% of a business's PCs are not in compliance at any given time.[23] Adding to this problem is the difficulty in getting accurate software inventories. For example, software inventories

Positive ROI of 294% realized over 3 years[19]

EDS is a leading global technology services company with 130,000 employees. The company delivers IT and business outsourcing services to clients in a variety of industries, such as manufacturing, health care, communications, government, and consumer retail.

Recently, EDS conducted an ROI analysis of Intel vPro technology at an EDS-managed call center located in Canada that supports three major clients across financial services, retail, and government. Results of the analysis showed substantial benefits:

- **Estimated positive ROI of 294% over 3 years** with a break-even at two years, when deploying PCs with Intel vPro technology.
- **Estimated savings of nearly $320,000 in 3 years** through reduced deskside visits and improved productivity of existing desktop support staff.
- **Productivity benefit equivalent to $440,000 across 3 years** since call-center employees can take more calls per agent each year, because Intel vPro technology enables off-hours patching.
- **Reduced power consumption by 25%** through the ability to remotely turn PCs on/off and remotely power them back up via Intel vPro technology to ready systems for the next work shift.

The ROI analysis shows how Intel vPro technology can significantly help enterprise save time and money, realize ROI on their technology investment in a short period of time, and at the same time, extend their remote management capabilities.

Save on power bills with better power management

IT technicians can now schedule PCs to be powered down overnight, and use Intel vPro technology to securely and remotely power up the PC from the service center to perform work off-hours or simply ready the PC for the next work shift.

Power savings: Siemens study

Siemens conducted a study of power savings using desktop PCs with Intel vPro technology. In the study, PCs were scheduled to be powered down for 8 hours per night. The study showed that, using Intel vPro technology for an IT infrastructure of 5,000 desktop PCs, Siemens could:

- Save 1.28 KWh per PC per day.[22]
- Save $52.80 per PC per year.[22]

"This one feature alone saves the company $264,000 yearly [and] pays for the cost of adding Intel vPro processor technology."[22]

– Siemens IT Solutions and Services newsletter, 2007

for notebooks are often up to 11% inaccurate.[24] One problem with inaccuracies caused by underreporting is that it may also expose corporate officers to liabilities, such as noncompliance with government regulations. There is a critical need for accurate system inventories, especially for PCs that are powered off or whose OS is inoperative.

PCs with Intel vPro technology give authorized technicians access to critical system information virtually anytime. This information is stored in protected, persistent memory (memory not on the hard drive) to improve discovery and inventory tasks. System information includes:

- **UUID**, which persists even across reconfigurations, reimaging, and OS rebuilds.
- **Hardware asset information**, such as manufacturer and model information for components. This information is automatically updated each time the system goes through POST.
- **Software asset information**, such as software version information, .DAT file information, pointers to database information, and other data stored by third-party vendors in the persistent memory space provided by Intel vPro technology.

With Intel vPro technology, IT technicians can:

- Write asset and other information (or pointers to asset information) into protected memory.
- Poll both wired and wireless systems in any power state for hardware and software asset information stored in protected memory – an OOB process that is up to 94% faster than performing a manual inventory.[18]
- Identify noncompliant PCs even if management agents have been disabled.
- Power up PCs that are off to perform inventory tasks, push replacement management agents to the system, and remotely power the PC back to the state in which the user left it.
- Push replacement agents to a wired or wireless PC, to bring it back into compliance before further network access is allowed even if management agents are missing.

The capabilities help reduce time-consuming manual inventories, saving significant costs in labor. Unused software licenses can also be appropriately reallocated to other resources, while hardware assets can be better utilized and warranties better managed. At the same time, businesses can be more confident that their audits are in compliance with government regulations.

Virtualization:
Next-generation standard practices for management, security, and cost reduction

As hardware technology evolves and use cases shift to meet emerging needs, virtualization has become a critical tool for both management and security. From a traditional model of multiple OSs, virtualization has become the next-generation standard practice for delivering OSs and applications to business PCs. PCs with Intel vPro technology are already designed to support these next-generation practices through Intel Virtualization Technology (Intel VT).[5]

Virtualization defined

In virtualized systems, multiple OSs with their associated applications can run simultaneously inside "virtual machines." Each virtual machine is a separate environment. Inside each environment, software can run in isolation from the other virtual machines on the system.

In traditional virtualization, isolation of each environment is achieved by introducing a layer of software below the OSs. This software layer is called a Virtual Machine Monitor (VMM). In traditional and application virtualization, the VMM abstracts each virtual machine away from the physical hardware, manages memory partitions for the virtual machine, and intermediates calls for shared hardware resources, like graphics, hard drives, and networking.

In next-generation virtualization, the OS can be abstracted (but still installed on the client PC) or streamed into a temporary, as-needed virtual "container" on the client PC. The temporary container isolates, protects, and allows the management of specific OSs and/or applications as long as the user needs that software streamed into the system. When the user no longer needs that OS or application, the streaming stops, and the virtual container is erased.

Usage models

Virtualization can be used to support next-generation, emerging, and traditional usage models for OSs and applications:

- Delivery of managed applications on-demand
- Delivery of managed desktop images
- Isolation of execution environments
- Traditional, multi-OS usage model

Virtualization: Streaming

Streaming refers to sending software (an OS or applications) over the network for execution on the PC (see Figure 8). During streaming, the software is sequenced, then divided into blocks and prioritized, and then placed in specific order for streaming. This allows the software to launch and begin operations on the PC even before all the code is streamed, so that users still have the responsiveness and performance of local execution. For IT, the advantage is that the OS and/or applications can be managed centrally, and standardized policies can be set to govern data storage. Since streamed software executes on the client, IT does not have to absorb the large data center build-out required by server-side compute models. Also, users enjoy the more responsive application experience of local software execution.

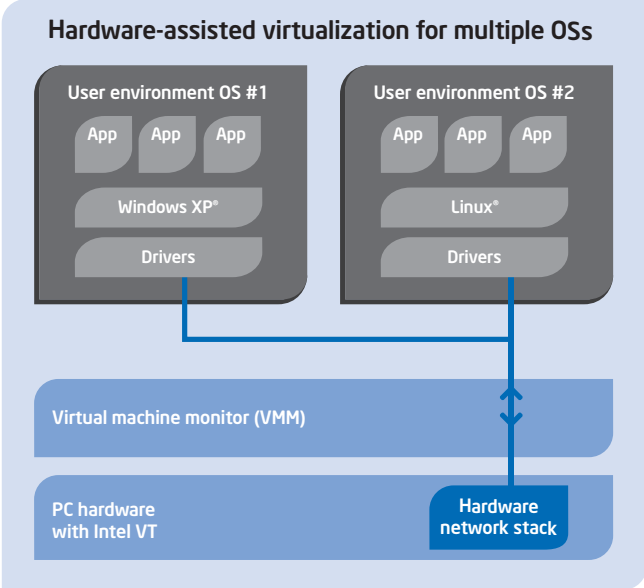

Figure 7. Hardware-assisted virtualization. Virtualization provides IT with isolated, secure spaces in which to abstract or stream OSs and applications. Both next-generation and traditional virtualization is supported on notebook and desktop PCs with Intel® vPro™ technology.

- **OS and application streaming:** the OS and applications are not installed locally. Instead, the OS and applications are streamed to the PC across the network. Critical application data can be stored at the data center, traditional problems with OS and/or application corruption are remediated by simply re-streaming the "gold" software image. Security, patching, and other IT services are also simplified, since they are performed only on the software image at the data center.
- **Application streaming:** the OS is installed locally, but the applications are streamed on-demand from the data center to the user. Data can be stored locally or at the data center, based on IT policy. Streaming only the applications reduces the network load, as opposed to streaming both the OS and applications. Also, applications can be cached for off-network use on mobile notebooks.

The terms "application streaming" and "application virtualization" are sometimes used interchangeably, but they are different. Streaming is the technique to deliver applications over the network.

Application virtualization is a technology that abstracts the application from the OS. Virtualized applications have full access to OS resources, but do not install themselves in the OS registry or system files. This can reduce many of the management issues and application conflicts that result from traditional installation.

PCs with Intel vPro technology support both OS streaming and application streaming. Application streaming products are available from several software vendors. OS streaming applications from software vendors are not yet available for mobile PCs.

Virtualization: Virtual containers

Virtual containers are self-contained virtual machines on the local PC. Virtual containers let you create individual, isolated work environments for a variety of scenarios. (see Figure 8). You can also use a managed virtual container to fully isolate and protect corporate data from personal data. This would allow you to increase security as necessary for sensitive information without frustrating users in their personal use of the system.

With virtual containers, the PC has at least one fully featured OS, and one or more additional, environments that are self-contained and used for specific purposes. For example, you could:

- Use virtual containers to separate locked-down corporate applications from more loosely-governed personal applications.
- Deploy a highly managed, limited-access image to a contractor or temporary employee.
- Allow employees to bring their own laptops into the office and use a managed virtual container to provide their applications. The virtualization software would abstract differences in the hardware, reducing the burden of validating the corporate image against the myriad of hardware combinations employees might be using.

Virtualization: Multiple OSs (traditional model)

The traditional model of virtualization gives the user access to multiple fully functional OS environments running in separate virtual machines. For example, the PC could have Microsoft Windows XP* and Linux* running side-by-side. This type of virtualization is also seeing significantly improved performance from the recent advances in Intel VT.

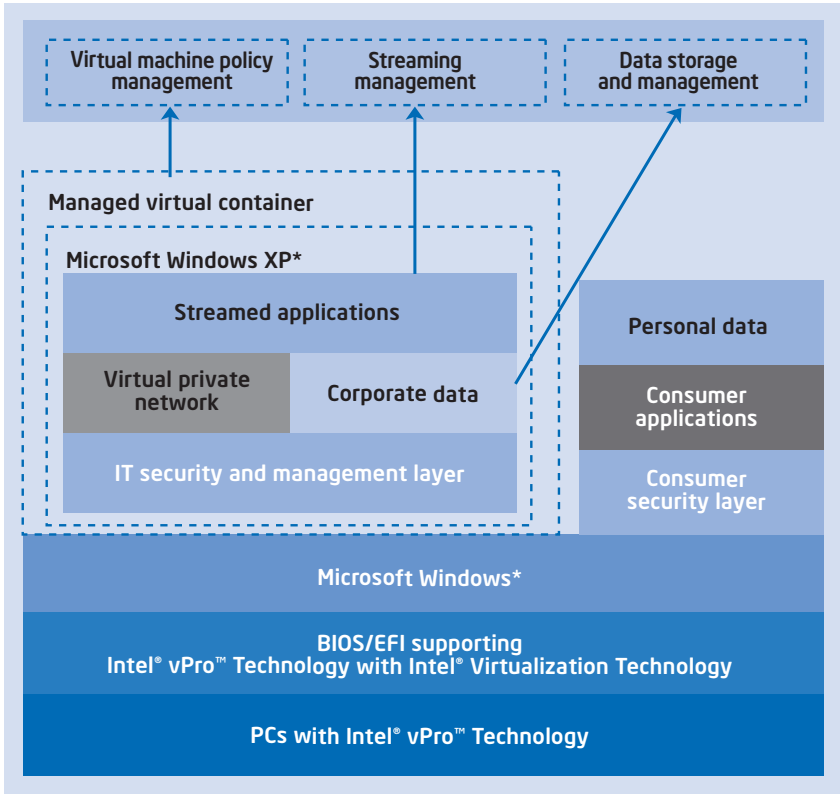

Figure 8. Application streaming. Intel® Virtualization Technology supports OS and application streaming, a next-generation standard practice for managing, securing, and delivering applications to users.

Dynamic Virtual Clients

PCs with Intel vPro technology can help IT organizations make progress against security and TCO challenges through a highly managed, centralized application delivery solution that complements their investment in Intel vPro technology. Solutions such as application streaming and virtualization, OS streaming, and virtual containers help IT centralize administration of application delivery and data security policy, but distribute the computation to the PC client. IT gets the control they need without the large data center build-out of server-based compute models. At the same time, users still enjoy application responsiveness and mobility. Together, dynamic virtual client solutions and Intel vPro technology provide a potent management, security, and TCO combination.

Traditional virtualization has typically been used:

- By software developers and support staff who need to work in more than one OS environment but do not want more than one PC on their desk.
- For OS migration, by keeping unportable legacy applications running in an earlier OS, while moving the rest of their applications over to Windows 7 or Windows Vista.

Traditional virtualization usually requires that you install a VMM software package from a vendor like VMware or Parallels, then build OS and applications images on top of the VMM software.

Intel VT is enabled today in VMM packages from vendors such as VMware and Parallels.

Intel® Virtualization Technology (Intel® VT) features

Today, virtualization can be achieved entirely with software – but this approach has traditionally had several challenges, including too much overhead, poor performance and unenforced isolation (a security issue).

Intel VT includes hardware enhancements that shift much of the burden of software-based virtualization into the hardware. This simplifies and reduces the overhead of virtualization, making it easier for third-party vendors to build lightweight VMMs. It also helps make virtualization more efficient and secure in general, and significantly improves performance – to near native levels or better, depending on the virtualization model.

Improving isolation and security

Intel VT includes hardware enhancements that virtualize memory, the CPU, and directed I/O. These features provide a significant level of hardware enforcement for the VMM's memory manager, and significantly improve isolation of the virtual environment. In turn, this helps improve security for critical processes and sensitive data.

Establishing a trusted execution environment

One of the persistent challenges of virtualization is ensuring the integrity of the VMM. Intel Trusted Execution Environment (Intel TXT) addresses this important security issue using a hardware-rooted process that establishes a root of trust, which allows software to build a chain of trust from the "bare-metal" hardware to a fully functional VMM. Using hash-based measurements protected by hardware, Intel TXT can detect changes to the VMM during its launch, which helps ensure that virtual machines will run as expected. The process allows the VMM to be verified earlier than with current software protection mechanisms (such as virus detection software).

Intel TXT also protects secrets (security credentials) during power transitions. With Intel TXT, during OS and application launch, passwords and keys are stored in protected memory. When the PC is rebooted, Intel TXT detects that secrets are still stored in memory, removes the secrets, then allows a normal boot process. (Secrets are not removed by Intel TXT after a normal protected partition tear-down. Removal of secrets under normal shutdown is handled by the VMM.) With Intel TXT, secrets that have not traditionally been protected before the OS and security applications are launched, are now protected even after improper shut-downs and in the traditionally vulnerable state before the OS and applications load once again.

Intel TXT is available in the latest notebook and desktop PCs with Intel vPro technology.

The future of virtualization

In terms of management, security, and delivery of applications, IT has traditionally considered hardware and software as bundled together. Next-generation use cases and corresponding evolutions in hardware are forcing a radical change in that view. As more and more software can be abstracted or streamed to a PC as a hardware-independent process, the link between hardware and software will become more perception than requirement.

What does this mean for virtualization? And what does this mean for IT? First, it means that managing, securing, and delivering software can be a simpler process, as can managing and supporting the hardware system. Intel vPro technology with Intel VT brings the best of isolation, security, and manageability for both software and hardware into one realm. Intel VT and next-generation virtualization

usage models will allow IT to manage software more distinctly. At the same time, the out-of-band capabilities of Intel vPro technology will continue to let IT manage the PC client regardless of the state of the OS, presence of management agents, or PC power state. The third-party management application extends IT functionality to the full enterprise.

- Manage and deliver applications — Virtualization, through Intel vPro technology with Intel VT.
- Manage and support the client PC — Intel vPro technology.
- Manage the enterprise — Third-party management application.

With virtualization, IT can concentrate on the specific aspect of security, maintenance, or management needed, based on their infrastructure and users. Eventually, users should be able to choose the PC configuration and hardware they prefer, and IT will simply deliver the OS and applications as needed for user workflow, as well as IT tasks.

Intel® VT compatible with other technologies

Standard memory, storage, and graphics cards work with Intel VT.[5] The latest notebook and desktop PCs with Intel vPro technology can also run most off-the-shelf OSs and applications without IT administrators having to perform special installation steps. The hardware-based virtualization technology is also designed to work with and complement other advanced security and management technologies from Intel, such as Intel Active Management Technology (Intel AMT).

Roadmap for virtualization technology

Table 8 briefly lists the virtualization technologies available in notebook and desktop PCs with Intel vPro technology.

Intel VT is enabled in VMM packages from vendors such as VMware. Intel VT with Intel TXT is available from vendors such as Green Hills Software. Intel VT including Intel VT for Directed I/O are enabled in VMM packages from vendors such as VirtualLogix. Intel VT including Intel VT for Directed I/O and Intel TXT are enabled in VMM packages from vendors such as Parallels.

Simplify and speed up configuration

Intel vPro technology allows powerful out-of-band access and management of PCs. To maintain the proper level of security for these capabilities, it is important that IT administrators establish the security credentials for Intel AMT appropriately for deployment into their service environment before configuring Intel AMT for remote management.

The configuration process may be accomplished with various levels of automation, as well as various levels of security by using certificates and keys or other credentials to secure the communication channel between the management console and the PC being configured. With these options for deployment, IT administrators can choose the level of security and automation appropriate for their network environments.

Methods to establish security credentials on Intel vPro technology PCs

Intel vPro technology supports different processes for setting up security credentials on the PC and management console. These processes allow you to select the security level appropriate for your environment:

- **One-touch manual:** Manually enter key pairs into the PC and the management console.
- **One-touch USB key:** Keys can be generated on the management console and stored on a USB key. The USB key is then used to install the keys onto the PCs.
- **Remote configuration:** Setup of initial security credentials occurs automatically (the PC must be configured by the original equipment manufacturer, or OEM) for remote configuration. Remote configuration requires a provisioning service, called a setup and configuration application (SCA). An SCA is required for both standard and advanced provisioning.

Table 8. Virtualization support in notebook and desktop PCs

Advanced technology	Offers	Intel® Centrino® 2 with vPro™ technology	Intel® Core™2 processor with vPro™ technology
Intel® VT	Virtualization of processor and memory	Yes	Yes
Intel® VT for Directed I/O	Virtualization of I/O hardware	Yes	Yes
Support for virtual containers	Temporary virtual machines that isolate streamed OS and applications	Yes	Yes
Intel® TXT	Trusted launch of the VMM and protection of secrets during proper or improper shutdown	Yes	Yes

Configuration models for PCs with Intel vPro technology

Intel vPro technology supports three configuration models to allow for flexible deployment (see Table 9):

- **Basic configuration** refers to a manual provisioning method useful for small businesses. It uses HTTP Digest for user authentication. There is no encryption applied to management traffic.
- **Standard configuration** provides enough security for most corporations. Client authentication is based on HTTP Digest which requires a user name and password. There is no encryption applied to management traffic.
- **Advanced configuration** provides the highest level of security features. This model allows you to configure Intel vPro technology-based PCs to use network access control standards such as 802.1x, Cisco SDN, and Microsoft NAP. You can also configure the management traffic to be encrypted with TLS or mutual TLS. In addition, authentication can be managed by the Microsoft Active Directory via Kerberos. These features can be remotely configured on Intel vPro technology-based systems. Not all management console vendors provide support to configure all security options.

General provisioning process

Provisioning a PC with Intel vPro technology generally follows three steps: setup, configuration, and integration. Setup establishes the initial security credentials required for secure communication between the setup-and-configuration application (SCA, which is used for standard and advanced configuration) and Intel AMT on the target PC. Setup also establishes the initial network and operational parameters required to begin configuration. Configuration is a self-initiated, automated step that depends on security credentials being in place. Integration means discovering and integrating the Intel vPro technology-based PC into the management application.

Full deployment typically consists of:

1. **Establish the management console,** including the SCA.
2. **Establish/enter certificates (standard or advanced configuration) or unique key pairs (basic configuration):** Create and establish security credentials and load them (automatically or manually) into each target PC. After security credentials are established, as soon as the PC is plugged into a power source and connected to the network, the PC can continue its own self-initiated configuration as a remote, fully automated process.
3. **Integrate** the Intel vPro technology-enabled PC into the management application and the management domain.

Table 9. Three configuration models.

Capability	Basic	Standard	Advanced
Intel® vPro™ technology features available	All	All	All
Configuration mode	SMB	Enterprise	Enterprise
Provisioning method	Manual	▪ Automated: remote via certificates, or "one-touch" USB-key ▪ Manual	▪ Automated: remote via certificates, or "one-touch" USB-key ▪ Manual
Provisioning service (SCA)	No	Yes	Yes
Deployment	One-to-one	One-to-many	One-to-many
Required enterprise infrastructure	▪ DNS and DHCP typical	▪ DNS and DHCP ▪ Provisioning service	▪ DNS and DHCP ▪ Provisioning service ▪ Active Directory integration (optional) ▪ Certificate authority (optional)
Authentication security	▪ HTTP Digest	▪ HTTP Digest	▪ HTTP Digest ▪ Kerberos (optional)
Management traffic encryption	No	No	Digital certificates (optional)
Secure network connectivity	No	No	▪ 802.1x ▪ Cisco SDN* ▪ Microsoft NAP*
Active Directory*	No	No	Yes (optional)
TLS and MTLS support	No	No	Yes (optional)
Upgrade path	No	Remotely re-provision to advanced	N/A

When your business needs to respond, your PCs will be responsive

IT organizations typically serve two masters: IT itself, with its requirements for security, maintenance, management, and upgrades/migration; and users, with their requirements for performance. Today, there is a third, growing business concern: power consumption, not just because of battery life for notebooks, but because energy costs are a significant operating expense and companies have an ever-increasing corporate focus on environmental responsibility.

Enter dual-core and quad-core Intel Core 2 processors — the powerhouse in all PCs with Intel vPro technology. These CPUs deliver improved performance per watt, outstanding performance for multitasking, and support for future OSs — up to 30% faster when multitasking, and up to 35% faster performance on compute-intensive applications.[25]

Best for business: Improved performance, energy efficiency and eco-smart computing

- **64-bit multi-core Intel Core 2 processors deliver excellent performance per watt.** These processors are optimized for improved multi-tasking and multithreading with compute-intensive applications, and deliver significantly improved performance over previous-generation notebook and desktop PCs. IT technicians can now run critical IT tasks, such as virus scans and e-mail synchronization in the background without bogging down foreground user applications.
- **Energy efficiency, great battery life and eco-smart computing.** Advanced architecture, package design techniques, power coordination, and thermal technologies let Intel Core 2 processors operate at very low voltages and use power more efficiently, so less unnecessary heat is generated and less cooling required for these high-performance systems designed to help meet Energy Star requirements. In desktop PCs, the result is excellent performance in quieter, smaller form factors. Notebooks with Intel vPro technology not only consume less power, but also include a power-optimized chipset, DDR3 memory, a new sleep state, and improved battery technologies to deliver great battery life in thinner, more innovative designs. The latest PCs with Intel vPro technology are also designed using lead-free, halogen-free manufacturing processes.[26]
- **Optional Intel® Turbo Memory for notebooks.** Intel® Turbo Memory stores large amounts of information closer to your processor to help reduce boot time and enable faster application loading when running Microsoft Windows Vista.[27]

IT administrators can now have the benefits of increased security and better remote management, while providing users with high-performance PCs that meet both wired and wireless needs.

Ready for the future

Notebook and desktop PCs with Intel vPro technology are stable, standardized platforms with broad industry support, ready for future operating systems and applications.

- **64-bit multi-core processor: Windows Vista and Windows 7 ready.** PCs with Intel vPro technology handle today's OSs and are ready for Windows Vista and Windows 7, which has a heavily threaded architecture, updated Windows Display Driver Mode (WDDM), built-in security features like Windows Defender,* BitLocker drive encryption,[13] and other advanced features.[28]
- **Multithreaded CPU: Ready for Office 2007.*** Intel Core 2 processors provide the performance needed for the next-generation of Microsoft Office,* including the performance for intense, always-on (by default) text-based search indexing, which is heavily multithreaded.
- **64-bit graphics support:** No need for a discrete graphics card. PCs with Intel vPro technology have built-in 64-bit graphics for an outstanding Windows Aero* experience. There is no need for a discrete graphics card with these PCs.

Stable, standards-based, and with broad industry support

To help the industry get the most from its technology investments, PCs with Intel vPro technology are:

- **Built on standards.** Intel vPro technology is built on industry standards to give you many choices in selecting OEMs and software vendors. Some of the standards upon which Intel vPro technology is built include ASF, XML, SOAP, TLS, HTTP authentication, Kerberos, DASH, and WS-MAN.
- **Broadly supported by the industry.** Intel vPro technology is supported by major software vendors in security software, management applications, and business software. PCs with Intel vPro technology are available from leading, worldwide desktop and notebook OEMs and are supported by major IT service providers and managed service providers.
- **Stable and simple.** The latest PCs with Intel vPro technology are available under the Intel® Stable Image Platform Program[12] (Intel® SIPP), so businesses can avoid unexpected changes that might force software image revisions or hardware requalifications. With Intel SIPP-compliant notebook and desktop PCs, IT can be more assured of having a stable platform that simplifies the deployment of new computing systems.

Wired or wireless: Security and manageability on the chip

Intel is uniquely positioned to provide critical business and IT capabilities on a notebook or desktop PC through extensive, breakthrough research and development, leading-edge manufacturing, and a unique ability to catalyze broad ISV support for creative solutions.

For IT organizations, the result is a professional-grade system designed from hardware to software with proven, built-in capabilities that resolve the most critical challenges of business and IT: improved, proactive security and remote manageability with energy-efficient performance. With Intel built in, IT organizations can address a wider range of enterprise needs and shift resources from managing and securing their notebook and desktop PCs, to accelerating business into the future.

To learn more about the built-in security and remote manageability capabilities of notebooks and desktop PCs with Intel vPro technology, visit www.intel.com/vpro.

Blog with the pros who have deployed Intel vPro technology, visit www.intel.com/go/vproexpert.

[1] Intel® vPro™ technology includes powerful Intel® Active Management Technology (Intel® AMT). Intel AMT requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see http://www.intel.com/technology/manage/iamt/.

[2] Systems using client-initiated remote access require wired LAN connectivity and may not be available in public hot spots or "click to accept" locations. For more information on client-initiated remote access visit, www.intel.com/products/centrino2/vpro/index.htm.

[3] No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) for PC protection (also referred to as the 'poison pill' in some documents) requires the computer system to have an Intel® AT-enabled chipset, BIOS, firmware release, software and an Intel AT-capable Service Provider/ISV application and service subscription. Intel® AT (PC Protection) performs the encrypted data access disable by preventing access to or deleting cryptographic material (e.g. encryption keys) required to access previously encrypted data. ISV-provided Intel-AT-capable encryption software may store this cryptographic material in the PC's chipset. In order to restore access to data when the system is recovered, this cryptographic material must be escrowed/backed up in advance in a separate device or server provided by the security ISV/service provider. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel® AT functionality has been activated and configured. The activation process requires an enrollment procedure in order to obtain a license from an authorized security vendor/service provider for each PC or batch of PCs. Activation also requires setup and configuration by the purchaser or service provider and may require scripting with the console. Certain functionality may not be offered by some ISVs or service providers. Certain functionality may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof.

[4] Requires WiMAX service subscription.

[5] Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[6] Intel® processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See http://www.intel.com/products/processor_ number for details.

[7] Wireless connectivity and some features may require you to purchase additional software, services or external hardware. For references to enhanced wireless performance, refer to comparisons with previous-generation Intel® technology. Availability of public wireless LAN access points is limited, wireless functionality may vary by country and some hotspots may not support Linux*-based notebooks with Intel® Centrino®2 with vPro™ technology systems. See http://www.intel.com/products/centrino/ index.htm and http://www.intel.com/performance/mobile/benchmarks.htm for more information.

[8] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see http://www.intel.com/technology/security.

[9] 64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device drivers and applications enabled for Intel® 64 architecture. Processors will not operate (including 32-bit operation) without an Intel® 64 architecture-enabled BIOS. Performance will vary depending on your hardware and software configurations. Consult with your system vendor for more information.

[10] Enabling Execute Disable Bit functionality requires a PC with a processor with Execute Disable Bit capability and a supporting operating system. Check with your PC manufacturer on whether your system delivers Execute Disable Bit functionality.

[11] The original equipment manufacturer (OEM) must provide TPM 1.2 functionality, and the PC must be provisioned with Windows Vista* Enterprise or Windows Vista* Ultimate Edition. TPM may not be available in all countries.

[12] Check with your PC vendor for availability of computer systems that meet Intel® Stable Image Platform Program (Intel® SIPP) guidelines. A stable image computer system is a standardized hardware configuration that IT departments can deploy into the enterprise for a set period of time, which is usually 12 months. Intel SIPP is a client program only and does not apply to servers or Intel-based handhelds and/or handsets.

[13] Any disk encryption technology may limit certain remote management capabilities. See your software vendor for information on interaction of disk encryption software and remote management.

[14] Wireless access to the powerful capabilities of Intel® vPro™ technology requires WPA, WPA2/802.11i security.

[15] Source: "An Analysis of Early Testing of Intel® vPro™ Processor Technology in Large IT Departments;" Charles LeGrand, Tech Par Group and Mark Salamasick, Center for Internal Auditing Excellence, University of Texas at Dallas; commissioned by Intel, April 2007.

[16] Up to 5x better performance with optional Intel® Next-Gen Wireless N technology enabled by 2x3 Draft N implementations with 2 spatial streams. Actual results may vary based on your specific hardware, connection rate, site conditions, and software configurations. See http://www.intel.com/performance/mobile/index.htm for more information. Also requires a Connect with Intel® Centrino® processor technology certified wireless n access point. Wireless n access points without the Connect with Intel® Centrino® processor technology identifier may require additional firmware for increased performance results. Check with your PC and access point manufacturer for details. (NOT for use in Russia, Ukraine, Bangladesh, and/or Pakistan).

[17] In order to experience the new benefits of wireless-n on notebooks with Intel® Centrino® with vPro™ technology, users must be connected to a wireless 802.11n network. Existing 802.11a, 802.11b and 802.11g networks/access points will not provide the new benefits.

[18] Results shown are from the 2007 EDS Case Studies with Intel® Centrino® Pro and the 2007 EDS case studies with Intel® vPro™ processor technology, by LeGrand and Salamasick., 3rd party audit commissioned by Intel, of various enterprise IT environments and the 2007 Benefits of Intel® Centrino® Pro Processor Technology in the Enterprise, Wipro Technologies study commissioned by Intel and may not be representative of the results that can be expected for smaller businesses. The EDS studies compare test environments of Intel® Centrino® Pro and Intel® vPro™ processor technology equipped PCs vs non- Intel® vPro™ processor technology environments. The Wipro study models projected ROI of deploying Intel® Centrino® Pro processor technology. Actual results may vary. The studies are available at www.intel.com/vpro, www.wipro.com, and www.eds.com.

[19] Source: EDS Intel vPro Call Center ROI Analysis, January 2008.

[20] Visit the Intel® Web site for case studies and proofs-of-concept listed under Explore the Ecosystem at: http://mysearch.intel.com/bizcontent/default.aspx?vs=&q=vpro& content Type=cs.

[21] Source: Reducing 856,000 Pounds of CO2 Emissions through Remote Services and Off-Hours Power Management , 2008, Intel. The study is available at http://communities.intel.com/servlet/JiveServlet/ previewBody/1703-102-1-2088/320101-001US_SOI_final061308.pdf.

[22] Source: Siemens IT Solutions and Services newsletter, 2007.

[23] Results shown are from the 2007 EDS Case Studies with Intel® vPro™ processor technology, by LeGrand and Salamasick., 3rd party audit commissioned by Intel, of various enterprise IT environments and may not be representative of the results that can be expected for smaller businesses. The studies compare test environments of Intel® vPro™ processor technology equipped PCs vs non- Intel® vPro™ processor technology environments. Tested PCs were in multiple OS and power states to mirror a typical working environment. Actual results may vary. The study is available at www.intel.com/vpro and www.eds.com.

[24] Results shown are from the 2007 Benefits of Intel® Centrino® Pro Processor Technology in the Enterprise, Wipro Technologies study commissioned by Intel and may not be representative of the results that can be expected for smaller businesses. The study models projected ROI of deploying Intel® Centrino® Pro processor technology Actual results may vary. The study is available at www.intel.com/vpro and www.wipro.com.

[25] Measured using SYSmark* 2007 Preview, BAPCo's latest version of the mainstream office productivity and Internet content creation benchmark tool used to characterize the performance of the business client, comparing latest generation comparing Intel® Centrino® 2 processor technology-based notebooks with comparable frequency first generation dual-core Intel Centrino processor technology based notebooks. SYSmark 2007 Preview features user-driven workloads and usage models developed by application experts. Actual performance may vary. See http://www.intel.com/go/consumerbenchmarks for important additional information.

[26] 45nm product is manufactured on a lead-free process. Lead-free per EU RoHS directive July, 2006 (2002/95/EC, Annex A). Some EU RoHS exemptions may apply to other components used in the product package. Residual amounts of halogens are below November 2007 proposed IPC/JEDEC J-STD-709 standards.

[27] Tests run on customer reference boards and preproduction latest generation Intel® Centrino® processor technology with optional Intel® Turbo Memory enabled against like systems without Intel® Turbo Memory. Results may vary based on hardware, software and overall system configuration. All tests and ratings reflect the approximate performance of Intel products as measured by those tests. All testing was done on Microsoft* Vista* Ultimate (build 6000). Application load and runtime acceleration depend on Vista's preference to pre-load those applications into the Microsoft* ReadyBoost* cache. See http://www.intel.com/performance/mobile/benchmarks.htm for more information.

[28] For information about system requirements for Windows Vista,* refer to http://www.microsoft.com/windows/products/windowsvista/buyorupgrade/capable.mspx.

*Other names and brands may be claimed as the property of others.

Printed in USA 0609/LKY/OCG/XX/PDF Please Recycle 311710-009US